**JP 56-156134 U**

Laid Open: November 21, 1981

Title: Random Number Generator Circuit

Utility Model Application No.: Sho 55-54192

Filed: April 21, 1980

Applicant: Nikoh Electronic Inc.

Claim 1:

A random number generator circuit, comprising:

a logical random number generator circuit;

a natural random number generator circuit; and

an arithmetic circuit that performs logical operation between an output from the logical random number generator circuit and an output from the natural random number generator circuit, wherein an output from the arithmetic circuit is output as a random number.

⑲ 日本国特許庁（JP）　　⑪実用新案出願公開

⑫ 公開実用新案公報（U）　　昭56—156134

| ⑤1Int. Cl.³ | 識別記号 | 庁内整理番号 |
|---|---|---|
| G 06 F 7/58 | | 7257—5B |
| G 09 C 1/00 | | 7368—5B |
| H 03 K 3/84 | | 6832—5J |

⑬公開　昭和56年(1981)11月21日

審査請求　未請求

（全 1 頁）

# ⑤4乱数発生回路

⑳実　　願　昭55—54192
㉒出　　願　昭55(1980) 4 月21日
㉑考　案　者　宮野正義
東京都港区芝白金 6 —16—42
㉑出　願　人　ニコー電子株式会社
横浜市港北区太尾町910番地
㉔代　理　人　弁理士　渡辺軍治

## ⑤7実用新案登録請求の範囲

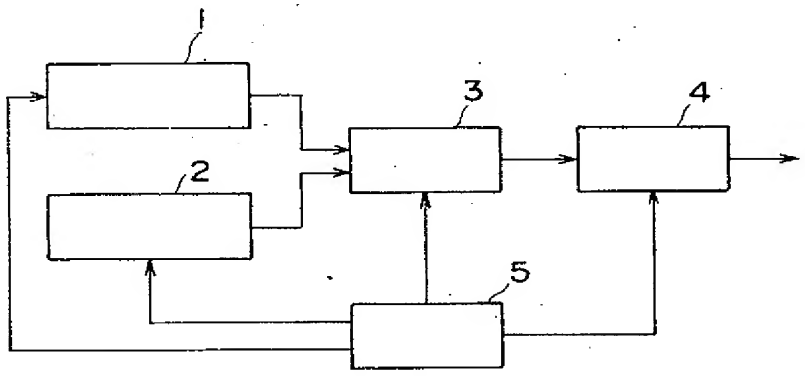
論理乱数発生回路と、自然乱数発生回路と、論理乱数発生回路の出力と自然乱数発生回路の出力とを論理演算する演算回路とを備え、演算回路の出力を乱数出力とすることを特徴とする乱数発生回路。

## 図面の簡単な説明

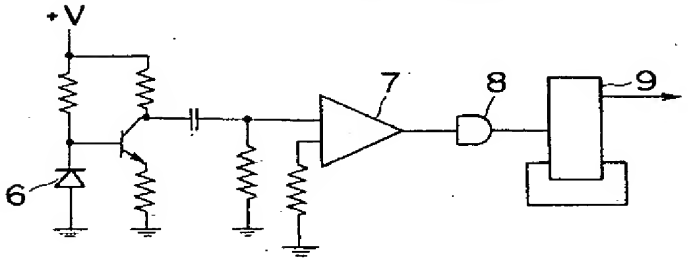
第 1 図は本考案の一実施例のブロック図。第 2 図は本考案の一実施例に用いる自然発生回路の一例の回路図。

1 ：論理乱数発生回路、 2 ：自然乱数発生回路、 3 ：半加算器、 4 ：記憶回路、 5 ：制御回路。

第1図




第2図



(4,000円)

# 実用新案登録願

昭和55年 4月21日

特許庁長官 川原能雄 殿

1. 考案の名称

ランスウハツセイカイロ
乱数発生回路

2. 考案者

ミナトクシバシロガネ
住所 東京都港区芝白金6－16－42
ミヤノ マサヨシ
氏名 宮野正義

3. 実用新案登録出願人

ヨコハマシコウホククフトオチヨウ
住所 神奈川県横浜市港北区太尾町910番地
デンシ
名称 ニコー電子株式会社
サクライ シゲキ
代表者 桜井茂樹

4. 代理人 〒166

住所 東京都杉並区高円寺南一丁目29番16号 TEL. 382—6771(代)
氏名 弁理士 (5654) 渡辺軍治

5. 添付書類の目録

| | | | |
|---|---|---|---|
| (1) ✓明細書 | 1通 | (3) ✓委任状 | 1通 |
| (2) ✓図面 | 1通 | (4) 願書の副本 | 1通 |
| | | (5) | 通 |

特許庁
55. 4. 22
出願第二課

✓ 55 054192

156134

# 明　　細　　書

1. 考案の名称

乱数発生回路

2. 実用新案登録請求の範囲

論理乱数発生回路と，自然乱数発生回路と，論理乱数発生回路の出力と自然乱数発生回路の出力とを論理演算する演算回路とを備え，演算回路の出力を乱数出力とすることを特徴とする乱数発生回路。

3. 考案の詳細な説明

本考案は暗号通信系などにおける信号を暗号化する符号変換器などに使用できる乱数発生回路に関する。

従来，前記符号変換器などに使用される乱数発生回路は論理乱数を発生する。論理乱数は予めその発生数列を予測することができ，復元性があるために符号変換器などに使用される。逆に言えば論理乱数は周期性を必然的に有するものであり，論理乱数で通信文を暗号化した場合，解読の可能性が存することになる。



15-6134

本考案は周期性を無くした乱数を発生する乱数発生回路を提供することを目的とし，この目的は論理乱数発生回路と，自然界に存在する雑音をピックアップしかつ波形整形して出力とする自然乱数発生回路と，論理乱数発生回路の出力と自然乱数発生回路の出力とを論理演算する演算回路とを備え，演算回路の出力を乱数列として用いることにより達成される。

以下，本考案を実施例により説明する。

第1図は本考案の一実施例のブロック図である。

1は従来から用いられている通常の論理乱数発生回路であり，2は自然界に存在する雑音，たとえば熱雑音，放射線雑音などをピックアップして波形整形して出力とする自然乱数発生回路であり，3は半加算器であり，4は半加算器3の出力を記憶する読み書き可能な記憶回路であり，5は論理乱数発生回路1，自然乱数発生回路2，半加算器3に出力してタイミングを合せて論理乱数発生回路1，自然乱数発生回路2からの出力を取り出し，半加算器3にて合成して記憶回路4へ出力して必

要ビット数だけ記憶回路4に記憶することを指令する制御回路である。

ここで自然乱数発生回路2はたとえば第2図に示す如く構成されている。

すなわち，6はツエナーダイオードであり，ツエナーダイオード6からの熱雑音を増幅器7で増幅し，増幅器7の出力はシユミツト回路8で波形整し，シユミツト回路8の出力をDフリツプフロツプ9にクロツクパルスとして入力し，Dフリツプフロツプ9の出力を図示しないシフトレジスタに入力し，シフトレジスタから制御回路5からの出力タイミングで取り出すように構成してある。

そこで論理乱数発生器1からの出力は自然乱数発生回路2からの出力は半加算器3で加算され，この加算値は記憶回路4に記憶され，たとえば通信文の暗号化に使用する。

また，たとえば2進化10進数を利用するものとすれば記憶回路4に記憶した半加算器3からの出力中，10進数10～15に対応する場合には記憶回路4からの出力時これを廃棄して新たに半加算

器3からの出力を取り入れ，10進数0～9に対応する場合にはこれを乱数列の一つの数値として送出するようにする。

以上は論理乱数発生回路1および自然乱数発生回路2が1組の場合の例について説明したが複数組を用いて合成してもよい。

そこで本考案によれば論理乱数発生回路のみによるときは前記した如き問題があるが，自然乱数発生回路の出力と論理乱数発生回路の出力とを演算したために論理乱数発生回路のみの場合の問題を解決し得る。また，自然乱数発生回路のみの場合は周期性は原則的には無いが，短期間においては出力値の発生頻度が片寄る可能性を有している。

しかし，これに論理乱数発生回路が演算されるため自然発生回路の上記欠点も解消される。

従つて，本考案によれば暗号通信系などにおける信号を暗号化する符号変換回路などに使用してきわめて有効で解読が困難となる効果もある。

4. 図面の簡単な説明

第1図は本考案の一実施例のブロック図。

第２図は本考案の一実施例に用いる自然発生回路の一例の回路図。

１；論理乱数発生回路。２；自然乱数発生回路。

３；半加算器。４；記憶回路。５；制御回路。

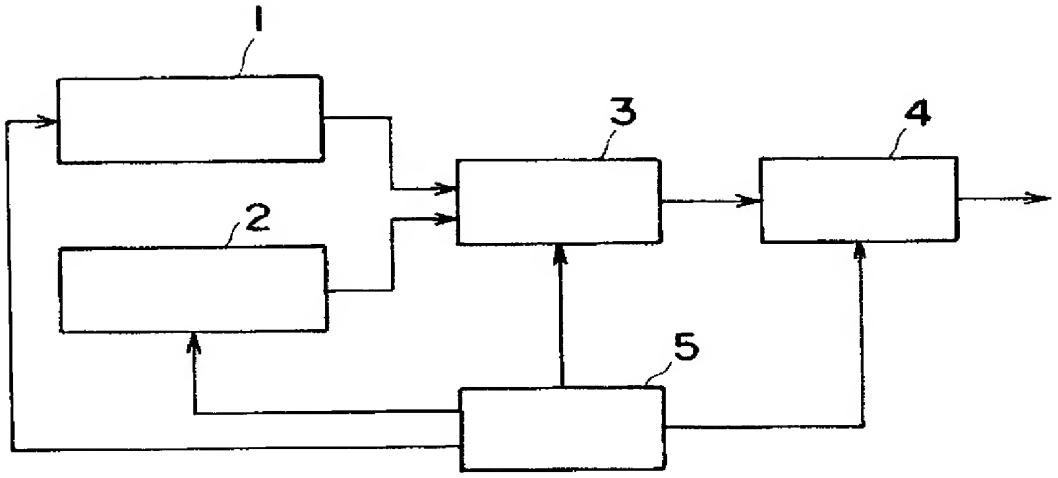
考案者　　宮野正義

出願人　　ニコー電子株式会社

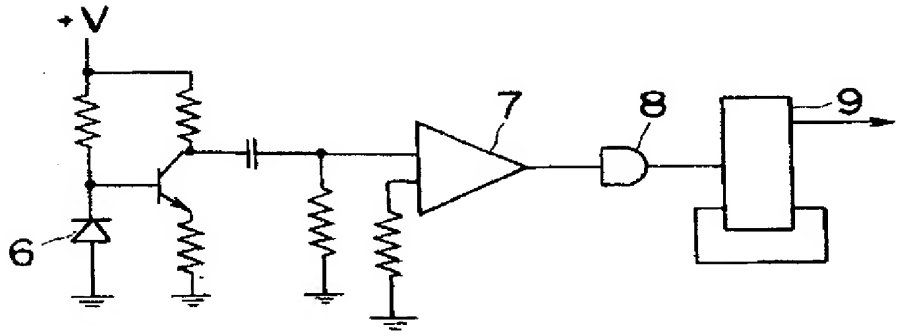
代表者　桜井茂樹

代理人　　弁理士　渡辺軍治

第1図




第2図




出願人 ニコー電子株式会社

代理人 弁理士 渡辺喜治